Maryland Official Use of Social Media Policy

Last Updated: 01/31/2017

Contents

1.0 Purpose

The Maryland Department of Information Technology (DoIT) is responsible for, and committed to, managing the confidentiality, integrity, and availability of the Executive Branch of Maryland State government Information Technology (IT) networks, systems, and applications.

This document establishes the DoIT policy for utilizing public **social media** for official communication. It incorporates best practices, acceptable use, and information management and control over State use of public social media platforms. The official use of social media allows State employees to build citizen and agency relationships, to provide timely and important updates to citizens, and to take part in national and global conversations relevant to the State.

2.0 Document and Review History

This policy supersedes the Maryland Information Security Policy v3.1 (2013) Section 12: Social Media Policy and any related policy regarding social media usage declared prior to the 2017 Cybersecurity Program Policy. This document will be reviewed annually and is subject to revision.

Date	Version	Policy Updates	Approved By:
01/31/2017	v1.0	Initial Publication	Maryland CISO

3.0 Applicability and Audience

This policy applies to all Maryland Executive Branch agencies and State employees assigned to use official social media accounts for purposes of communicating official state or agency information to the public.

4.0 Policy

The purpose of this policy is to provide rules of conduct for State organizations and State employees when using social media platforms to communicate in an official capacity on behalf of the State of Maryland. The Executive Branch expects all authorized **social media coordinators** to understand and to follow the requirements of this policy.

If an agency chooses to utilize a social media platform, the agency will designate the platform(s) for best representation of agency and State reputation and brand. Agencies will be expected to oversee and verify who may "speak" and what is "said" on behalf of the agency and the State.

4.1 Social Media for Official Use Only

Social media platforms will be used only for official, informal public communications intended as informational updates related to ongoing issues, engagement with the public, or agency specific information (e.g. inclement weather alerts and closures, public utilities status updates, and annual agency-hosted events). These public social media channels are intended only for

informal communications. All communications with legal and policy effect will be handled through more formal, State-owned channels.

State officials may have account types with varied disclosure requirements as shown in the table below. Accounts will be centrally created and managed in accordance with the current *Account Mangement Policy* and access controls.

#	Media Account Type	Requirements For Account Use
A	Individual – Official Account	Individual communication originating from a State employee conducting State business on a State-controlled social media account. The State employee must disclose the following information within their communication: ▪ First and last name ▪ Contact information (at a minimum a State email address must be provided; additional information is permitted) ▪ Individual's organization (department or agency name)
B	Individual – Non Official Account	Individual communication originating from a State employee clearly representing themselves as a State employee, *but not conducting State business*, publishing content to any social media account outside of a Maryland domain. The State employee must include a disclaimer such as: ▪ "The postings on this site are my own and don't necessarily represent Maryland's positions, strategies or opinions."
C	Organization – Official Account	Organizational communication originating from a State organization controlled social media account. The State organization must disclose the following information whenever it uses the communication channel: ▪ Organization name and a single point of contact for inquiries about the communication (at the minimum, a general email address, additional information, such as the organization telephone number, is permitted).

4.2 Social Media Usage Requirements

The table below establishes the requirements for an agency's official use of a social media platform.

#	Name	Requirement
A	State CISO Notification	All Executive Branch agencies will notify the Director of Cybersecurity/State CISO of any agency social media accounts, including the name of the account, who is authorized to post, and the purpose of the account (State employee representation or State agency engagement).
B	Official Use Only	Any use for non-government business or intentional misuse of social media platforms will be considered a security violation.
C	Accountability and Ethical Use	State employees representing an agency or the State are responsible for the content they publish on social media sites (see Section 4.4)
D	Information Linking	Whenever possible, messages shall direct users to official channels such as agency web page announcements, official online forms, State or agency documents or online services necessary to conduct business with the State/agency.

#	Name	Requirement
E	Account Protection	All official social media accounts will be audited by the DoIT Information System Security Mananger (ISSM) and will adhere to the requirements in Section 4.7.
F	Continuous Monitoring	The DoIT Security Operations Center (SOC) will actively monitor social media accounts for indication of misuse or compromise.

4.3 Social Media Management

All Executive Branch agencies will manage their own official social media accounts and will be held responsible and accountable for its use. Each agency will provide the State CISO a list of all social media accounts to be audited periodically by the DoIT ISSM and actively monitored by the DoIT Security Operations Center.

Each agency will prepare an incident response plan (see *Cybersecurity Incident Response Policy*) for each social media platform in the event of a compromise, e.g. an account gets high-jacked or an unauthorized user gains access. The incident response plan will define the process for:

- Recovering the account
- Deleting the account
- Notificating all subscribers of the compromise

Each agency will ensure the immediate revocation of access by any user no longer authorized to publish to a social media platform (e.g., due to termination or relieving of social media duties). Agencies will protect accounts as directed in Section 4.7 and exercise due care and due diligence in ensuring proper use of social media platforms.

4.4 Social Media Ethical Conduct

In all social media use, the State employees and organizations will maintain professional behavior and conduct themselves according to the highest possible ethical standards. The table below describes the ethical conduct requirements.

#	Name	Requirement
A	Social Media Usage	All authorized social media users will be familiar and comply with the Terms and Conditions of the platform they are using.
B	Accurate Information	Authorized social media users will not knowingly communicate inaccurate or false information. All reasonable efforts will be made to verify facts and ensure status updates are accurate.
C	Confidential Information	Agencies will make every effort to prevent the inadvertent release of confidential information (see *Public and Confidential Information Policy*).
D	Agency and State Mission	Authorized users will remain focused on the State and agency missions, will address customer input professionally, and will engage customers with accurate and verified information.

4.5 Social Media Misuse

Any agency or State employee identified as misusing a social media platform will lose access to the account and the conduct will be treated as a security violation. The table below is a non-exhaustive list of examples of misuse.

#	Name	Example of Misuse Considered a Security Violation
A	Disregard of Agency or State Mission	Any authorized user sending or responding to private messages not related to agency or State mission or business.
B	Unprofessional Behavior	Any authorized user engaging in vulgar or abusive language, personal attacks, or use of offensive or demeaning language targeting individuals or groups.
C	Commercial Endorsements	No agency or State employee shall endorse or "sell" any commercial product, service, or capability.
D	Political or Religious Endorsements	No agency or State employees shall comment on, endorse, or engage in political or religious conversation.
E	Repost Content	Agencies or State employees shall not repost or forward content except official government or industry specific material. Preferably, references should link to official agency or State web pages containing the original content (e.g., a Governor's public statement or IRS Tax information for MD residents).
F	Lobbying or Charity Solicitation	No agency or State employee shall post content attempting to influence decisions made by officials in government or advertise any charity programs other than those officially endorsed by the State.
G	Unapproved Content	No agency or State employee shall post or refer to unapproved content, including commenting on unauthorized disclosure of information to a public forum, and instead will refer to any official statements, if available (e.g. if State proprietary information is posted in WikiLeaks the State will not acknowledge, discuss, or confirm or deny any information within a social media platform).

4.6 Content Moderating

In some social media formats, State employees may be responsible for moderating comments.

- Customer comments that are either positive or negative *and* in context to the conversation will be allowed to remain visible within the forum, regardless of whether it is favorable or unfavorable to the State.
- Comments that violate professional use, e.g., containing disparaging remarks of individuals or groups, racist/sexist remarks, or other vulgar content, may be removed from the forum to keep the discussion on-topic and relevant.

4.7 Social Media Account Protection

Social media accounts will be protected with enhanced security, described below, to restrict (malicious) access to or unauthorized use of the account and to ensure the account remains available:

#	Name	Requirement
A	ISSM Auditing	The DoIT ISSM or delegated ISSM will audit agency and State social media accounts for misuse and unauthorized disclosure.
B	Password Security	Agencies will ensure proper passwords are generated and meet the following requirements: ▪ 20 character passwords (due to direct exposure from the Internet this ensures unauthorized users cannot easily crack the password) ▪ At least 3 capital letters, 3 lower case letters, 3 numbers, and 3 special characters unless password constraints within the site prohibit these combinations (this helps to reduce possible password cracking). ▪ Changed immediately any time a user is no longer authorized to use that account. ▪ Dual Factor authentication wherever applicable and managed by the agency.
C	Change Notification	Agencies, the DoIT ISSM, and the DoIT SOC will update the State CISO upon any social media account violations or suspected compromises.

5.0 Exemptions

This policy is established for use within the DoIT Enterprise. If an agency under the policy authority of DoIT requires an exemption from this policy then that agency must submit a DoIT Policy Exemption Request Form and clearly articulate the reason for the exemption. An operational risk assessment will be conducted to identify the risks and the agency's mitigation strategy associated with this exemption. If the agency can accept the risk, an exemption to this policy may be granted.

6.0 Policy Mandate and References

The Cybersecurity Program Policy mandates this policy. Related policies include:

- Acceptable Use Policy
- Account Management Policy
- Auditing and Compliance Policy
- Continuous Monitoring Policy
- Cybersecurity Incident Response Policy
- Public and Confidential Information Policy

7.0 Definitions

Term	Definition
Social Media	Publicly available websites and applications that enable users to create and share content or to participate in social networking.
Social Media Coordinators	A State representative, agency-designated individual, or group authorized to use a social media platform for the purposes of informally providing information or status updates to the public.

8.0 Enforcement

All Executive Branch agencies will abide by the requirements within this policy and will be audited and monitored, by the Director of Cybersecurity/State CISO and DoIT, as described with Section 4.0. Oversight of social media use by agencies ensures the integrity and proper use of Maryland State information assets.

If DoIT determines that an agency is not compliant with this policy, the agency will be given a sixty (60) day notice to become compliant or at least provide DoIT a detailed plan to meet compliance within a reasonable time before the issue is reported to the Secretary of Information Technology. After such time, if the agency remains out of compliance the Secretary of Information Technology will be notified and remediation will be mandated.

Any attempt to circumvent the requirements within this policy, such as intentionally or inadvertently changing account information while accessing official agency social media accounts or misusing the platform as indicated in this policy, will be treated as a security violation and subject to disciplinary action which may include written notice, suspension, termination, and possible criminal and/or civil penalties.